イージスEWを活用された
お客様事例

2024/11/06
㈱未来研究所

イージスEWを活用されたお客様事例　概要

■イージスEW活用例

製造業から、運送、大学、web制作会社まで広く使っていただけている。

・電力系監視システム（特定社会基盤事業）・納品前システムの脆弱性診断テスト
・サブドメインを多数使用している中堅大学（2500アドレス）
・認証基盤提供SaaSベンダー（ユーザSaaSサービス・社内システム管理等の複数ドメイン管理）
・化粧品をODMの製造ラインを有している製造業（販売のための複数ドメインの一括脆弱性管理）

■訴求ポイント

・インターネット（ASM/ペネトレ）・イントラ、納品前脆弱性診断の事例（事例１）
・多数のサブドメイン・ケースについての事例（事例２）
・複数ドメインの一括管理（事例３）
・製造業でのコンサルティング事例（事例４）

イージスEWは、小規模LANレベルから大規模ユーザまで幅広くお使いいただいております。
また、お客様は「自社で登録したAEGIS-EWアカウント」で「自社用のダッシュボード」を運用できます。

事例１　電力会社向けシステム開発会社（特定社会基盤事業者）

事例１　電力会社向けシステム開発会社

■お客様の概要

お客様は、情報通信基盤向けコンサルティング、導入支援、
システム構築から運用保守までを手がける中堅SIerとなります。

株式会社　＊＊＊＊＊＊
資本金：　6億円
社員数：　400名

主な納入先：　大手電力会社、市役所、医療機関向けに納入。
音響通信システム開発に強みを持つ。

イージスEW導入の理由：
大手電力会社（特定社会基盤事業者）向けにシステム納入を
行うにあたり、脆弱性診断実施結果を求められたため。
なお、この診断はワンショット契約で行われました。

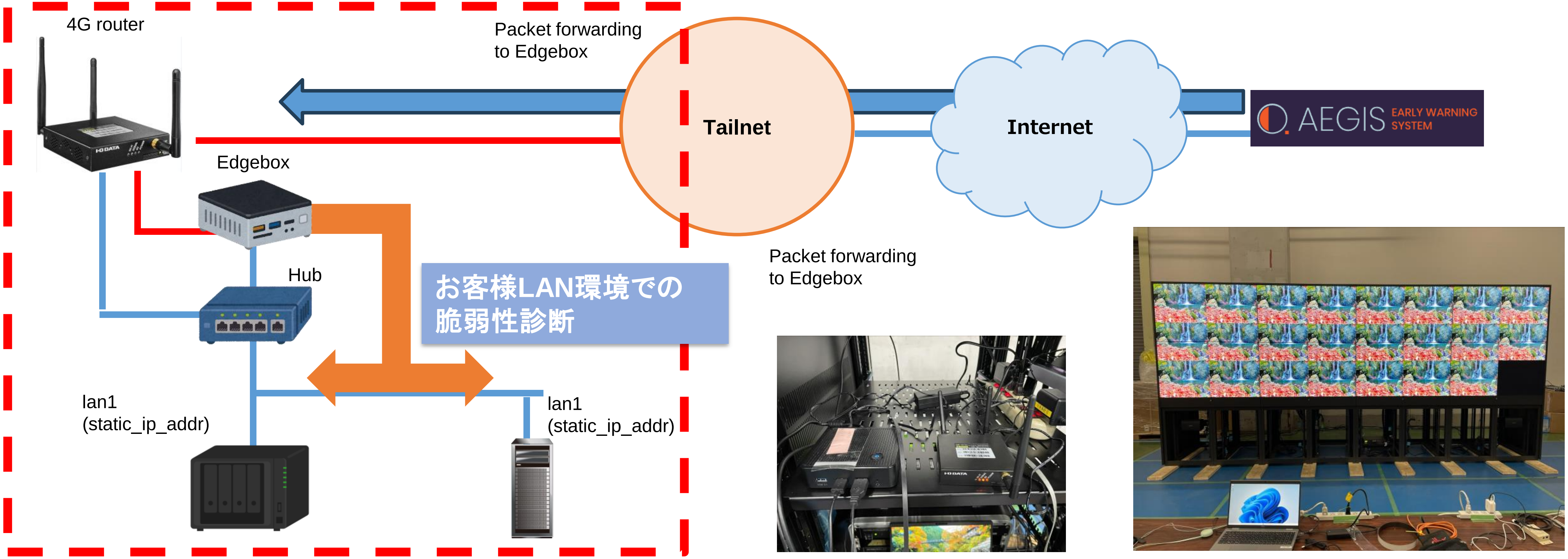
参考：
イージスEWによる脆弱性診断実施時の写真

事例１　電力会社向けシステム開発会社

未来研究所
Future Research Inc.

■脆弱性診断実施方法

４Gルータ付きルータを経由して、VPNを構築することにより、
お客様が構築したLAN環境（大手電力会社様への納品物）の脆弱性診断を行いました

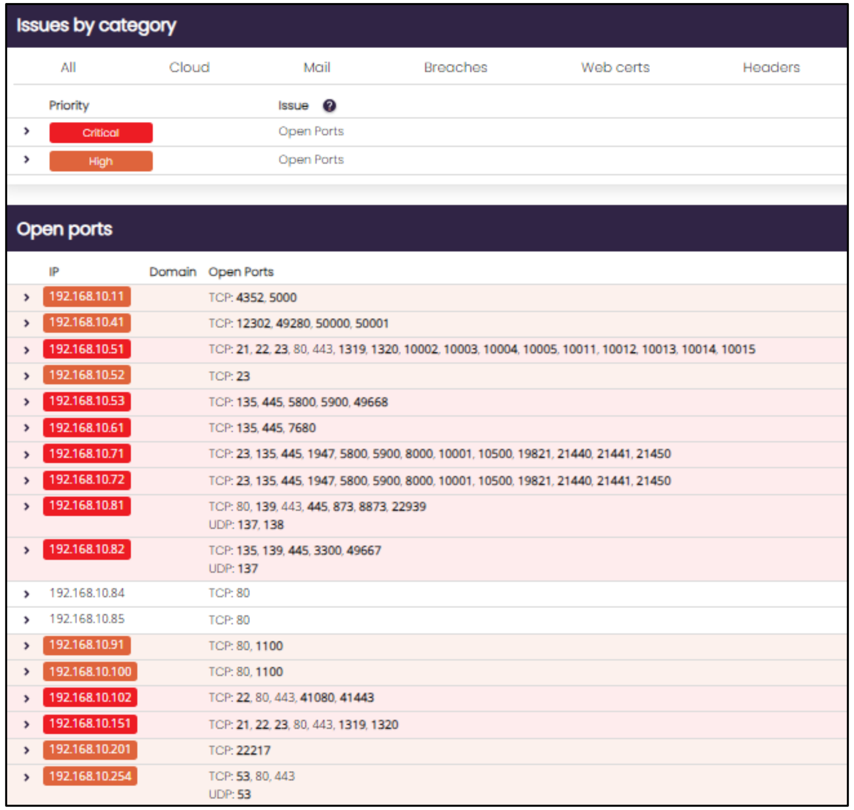


事例１　電力会社向けシステム開発会社

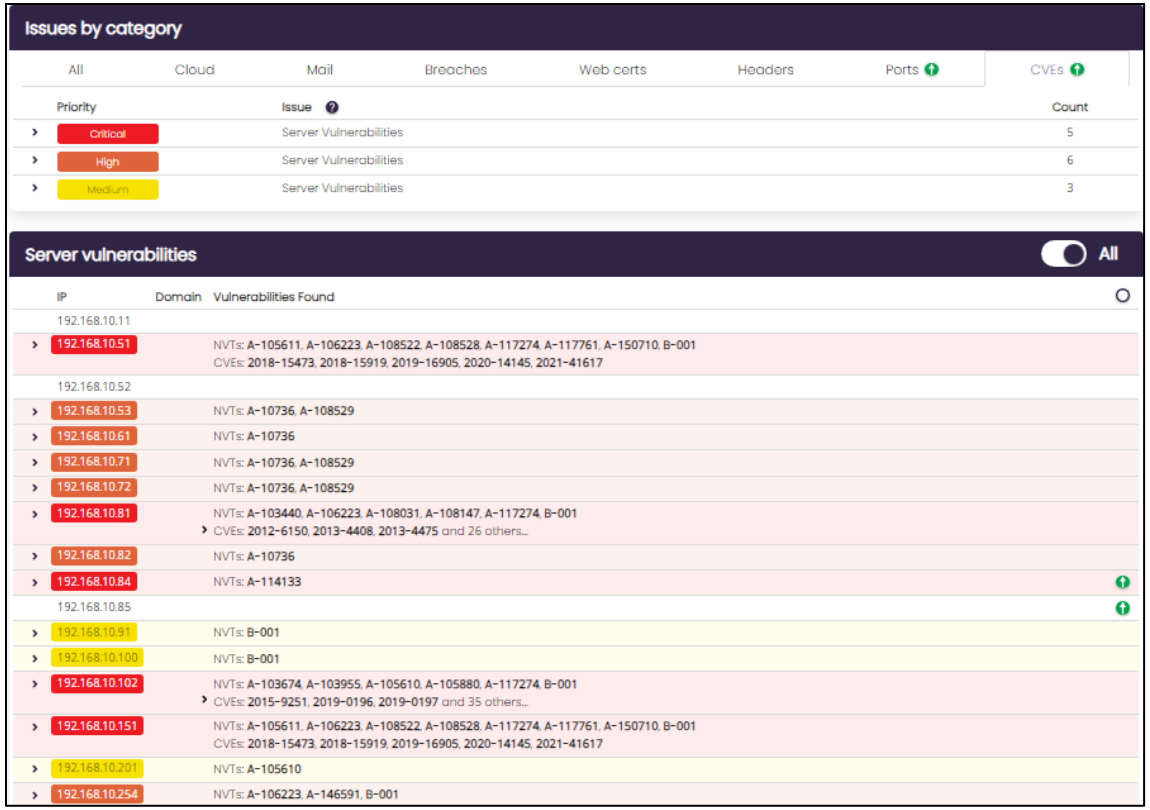
未来研究所
Future Research Inc.

■イージスEWによる診断内容

この導入事例では、IoT装置を中心とした内部ネットワーク向けの脆弱性診断となります。
グローバルネットワークに接続されていない環境のため、「ポート調査」「CVE調査」がメインとなります。



ポート調査



CVE調査

事例１　電力会社向けシステム開発会社

未来研究所
Future Research Inc.

■その後の導入結果

この脆弱性診断は、お客様が大手電力会社様へ納入するため
に行ったものです。
このイージスEW脆弱性診断により、

「納品前の不必要なポートの閉鎖」
「ファームウエアアップデートによるハードニング」

を行うことができました。

なお、このお客様からは、
別システムでも同様にイージスEWを用いた診断を
随時受注しております。

参考：
イージスEWによる脆弱性診断実施時の写真

事例２　中堅工学系大学様

事例２　中堅工学系大学様

未来研究所 Future Research Inc.

■お客様の概要

お客様は、地方都市に所在地がある中堅工学系大学様です。

大学名　＊＊＊＊＊＊工科大学
学生数：　2500名
サブドメイン数：約2500個
サーバー数：2300台

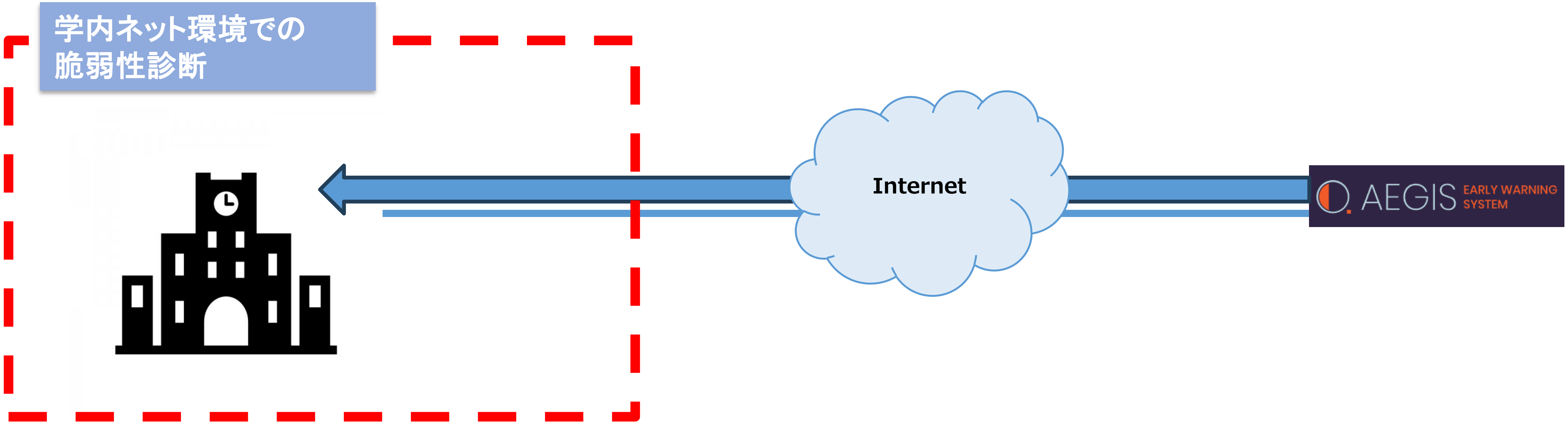
イージスEW導入の理由：
学内の所有サーバの脆弱性管理および、管理外端末を発見するため

（本事例の費用感：2499個のサブドメイン数におけるASM脆弱性診断料金　25万円（税抜き）／1回）

事例２　中堅工学系大学様

■脆弱性診断実施方法

脆弱性診断方法は、お客様の学内ネット環境に対して、イージスEWを実施しました。



**調査対象のサーバは、学内ネットワークに構築されており、
DNSサーバも学内で運用されています。**

事例２　中堅工学系大学様

■イージスEWによる診断内容

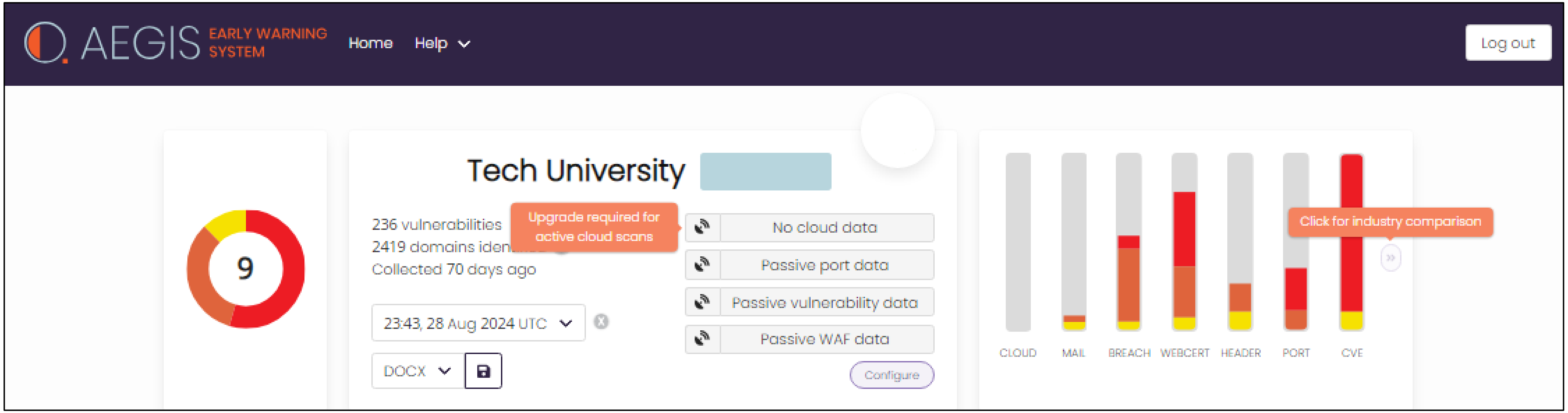
この導入事例では、AMSフルスキャンを行いました。
「メールなりすまし対策」、「データ侵害」、「サーバ証明書」、
「ポート調査」、「HTTPセキュリティヘッダ」、「CVE調査」を実施しました。

分野識別	Mail	送信ドメイン認証	「メールなりすまし」対策できているかどうか？
	BREACH	データ侵害	お客様のドメインで登録されたメールアドレスが、 ダークウェブに流れていないか？
	WEBCERT	Web認証関連	WEBサーバ証明書は正しいのか？
	HEADER	HTTP関連ヘッダー関連	HTTPセキュリティヘッダは正しく導入されているか？
	PORT	ポートスキャン攻撃	攻撃されやすいポートは開いていないか？
	CVE	共通脆弱性識別子CVE (Common Vulnerabilities and Exposures)	CVE脆弱性が残っていないか？

事例２　中堅工学系大学様

■その後の導入結果(1)

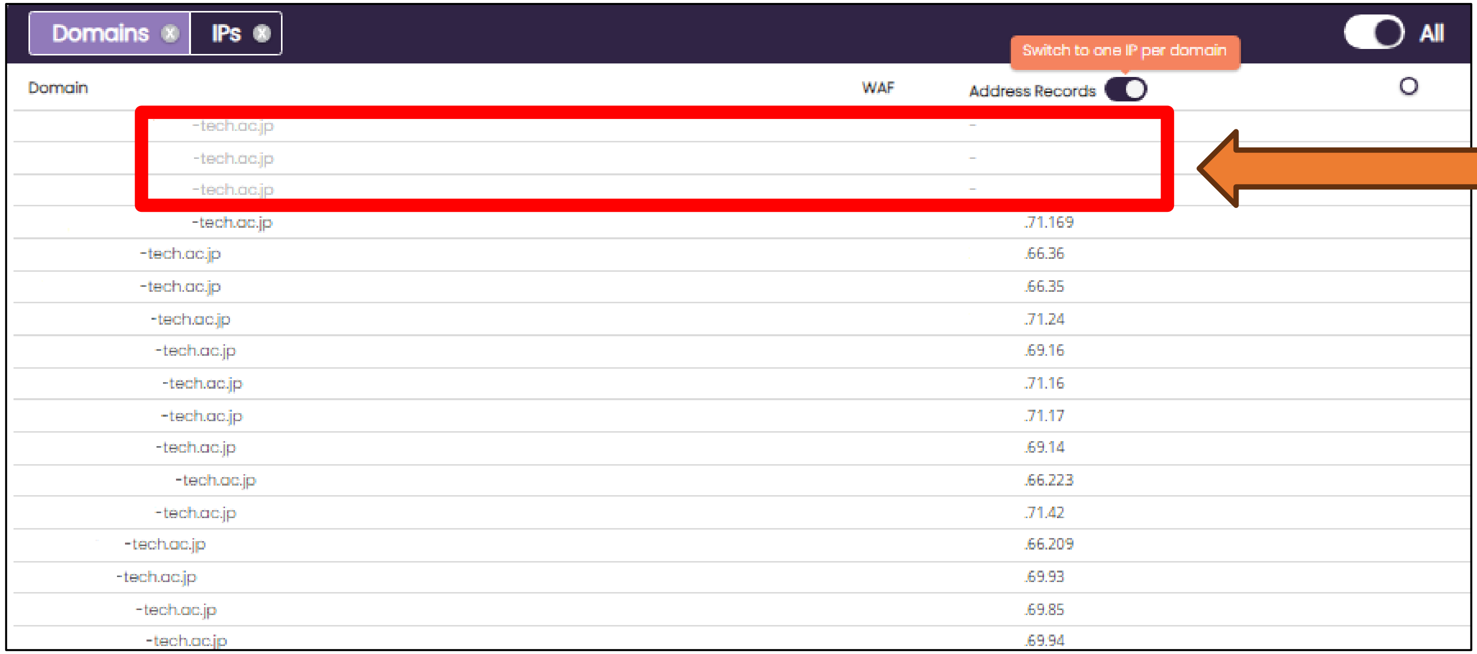
このお客様の場合、約2400ドメインにも渡る大規模なサーバ数を保有しております。
このような場合でも、イージスEWなら「他社製品よりも圧倒的な安さ」で脆弱性診断を実施可能です。



事例２　中堅工学系大学様

■その後の導入結果(2)

お客様保有のサーバは、2300台ほどあり、管理が困難状態でした。
イージスEWを導入することにより、使用していないサブドメインの管理も容易になりました。



使われていないサブドメイン・IPアドレスは灰色で表示されており、一目で「未使用のサブドメイン」を判別可能です

事例２　中堅工学系大学様

■その後の導入結果(3)

イージスEWの調査によって、すぐにでも乗っ取り可能な脆弱性があることが判明しました。
大学側の情報システム部門と当社にて連携を行い、改善の取り組みを行っています。

```
C:¥Users¥user>curl http://******.ac.jp --verbose --head
* Host ******.ac.jp:80 was resolved.
* IPv6: (none)
* IPv4: ******
*   Trying *****:80...
* Connected to ******.ac.jp (****) port 80
> HEAD / HTTP/1.1
> Host: *****.ac.jp
> User-Agent: curl/8.9.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 302 Found
HTTP/1.1 302 Found
< Date: Wed, 06 Nov 2024 04:20:45 GMT
Date: Wed, 06 Nov 2024 04:20:45 GMT
< Server: Apache/2.4.37 (AlmaLinux) OpenSSL/1.1.1k
Server: Apache/2.4.37 (AlmaLinux) OpenSSL/1.1.1k
```

「Apache web server」が明らかに古いままです。
■これらのモジュールは、重大な脆弱性をもったままです。

例：
・CVE-2021-44790（Apache httpd の重大な脆弱性）CVSS 9.8（緊急）
リモートコード実行可能な脆弱性
→Luaが有効になっている場合、乗っ取り可能です。

・CVE-2019-0211（Apache権限昇格の脆弱性）CVSS 7.8（重要）
ローカルユーザーから特権昇格
これは、著名な脆弱性であり、Exploit（侵入するためのコード）が配布されています。
https://github.com/ozkanbilge/Apache-Exploit-2019/tree/master/CVE-2019-0211-apache

これは、apacheユーザ権限を乗っ取った後、root権限に昇格するためのコードです。

事例２　中堅工学系大学様

■その後の導入結果(4)

イージスEWによる診断によって「学生向けに配布されたメールアドレスから、大量のデータ侵害」が発見されました。
学生はeメールアドレスを持っていないことが多く、大学で配布されたメールアドレスが使われていると判明しました。
イージスEWによる診断がきっかけで、データ侵害の被害に遭っている学生さんに向けて注意喚起を行うことになりました。

Data breaches All

実際のメールアドレス

Email Address	Company Breached	Date of Breach	Breached Information
	MGM2022Update	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	Gravatar	2020-10-03	Email addresses, Names, Usernames
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	MDPI	2016-08-30	Email addresses, Email messages, IP addresses, Names
	MDPI	2016-08-30	Email addresses, Email messages, IP addresses, Names
	OnlinerSpambot	2017-08-28	Email addresses, Passwords
	OnlinerSpambot	2017-08-28	Email addresses, Passwords
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	AntiPublic	2016-12-16	Email addresses, Passwords
	ExploitIn	2016-10-13	Email addresses, Passwords
	LinkedIn	2012-05-05	Email addresses, Passwords
	PDL	2019-10-16	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles
	YouveBeenScraped	2018-10-05	Email addresses, Employers, Geographic locations, Job titles, Names, Social media profiles
	Cit0day	2020-11-04	Email addresses, Passwords
	Collection1	2019-01-07	Email addresses, Passwords
	NotSOCRadar	2024-08-03	Email addresses
	TelegramCombolists	2024-05-28	Email addresses, Passwords, Usernames
	LinkedIn	2012-05-05	Email addresses, Passwords
	PDL	2019-10-16	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles
	Peatix	2019-01-20	Email addresses, Names, Passwords
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	MDPI	2016-08-30	Email addresses, Email messages, IP addresses, Names
	Gravatar	2020-10-03	Email addresses, Names, Usernames
	MGM2022Update	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	MGM	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses
	MGM2022Update	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses
	Adobe		
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	Dropbox	2012-07-01	Email addresses, Passwords
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	AntiPublic	2016-12-16	Email addresses, Passwords
	MDPI	2016-08-30	Email addresses, Email messages, IP addresses, Names
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	AntiPublic	2016-12-16	Email addresses, Passwords
	Collection1	2019-01-07	Email addresses, Passwords
	ExploitIn	2016-10-13	Email addresses, Passwords
	MDPI	2016-08-30	Email addresses, Email messages, IP addresses, Names
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames
	Adobe	2013-10-04	Email addresses, Password hints, Passwords, Usernames

Issues by category

All | Cloud | Mail | Breaches | Web certs | Headers | Ports | CVEs

	Priority	Issue	Count
›	Critical	Breached Emails	3
›	High	Breached Emails	33
›	Medium	Breached Emails	9

レポートより、多くのデータ侵害が発生していることがわかります

@ .ac.jp	NotSOCRadar	2024-08-03	Email addresses
@ .ac.jp	NotSOCRadar	2024-08-03	Email addresses
@ .ac.jp	NotSOCRadar	2024-08-03	Email addresses
@ .ac.jp	NotSOCRadar	2024-08-03	Email addresses
@ .ac.jp	TelegramCombolists	2024-05-28	Email addresses, Passwords, Usernames
@ .ac.jp	TelegramCombolists	2024-05-28	Email addresses, Passwords, Usernames

メールアドレス（ID）とパスワードがダークウェブに漏れていることがわかります。

事例3　SSO認証基盤サービス会社様

事例3　SSO認証基盤サービス会社様

■お客様の概要

お客様は、大学や病院、市役所向けのシングルサインオン環境を提供しているベンチャー企業様です。
なお、このお客様では複数のドメインを所有しており、一括管理を希望されておりました。

株式会社　＊＊＊＊＊＊
資本金：　1500万
社員数：　３0名

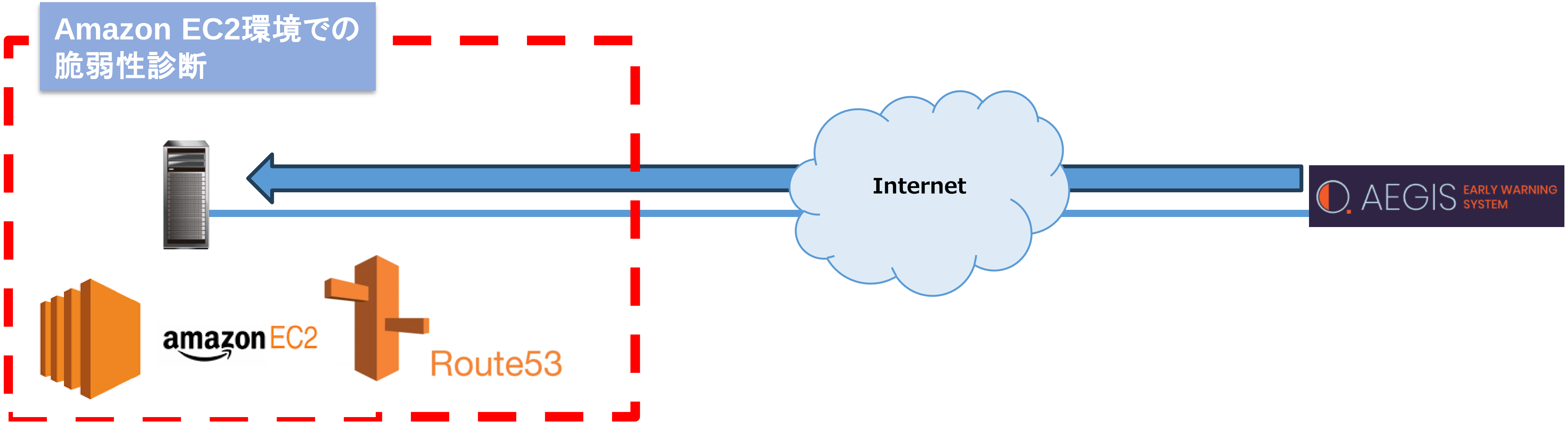
主な納入先：　大手大学（学生数：18,000名）、市役所けに納入。

イージスEW導入の理由：
自社サービスにおいてハードニングを実施するため。
毎月のASM診断を一年間契約しております。

事例3　SSO認証基盤サービス会社様

■脆弱性診断実施方法

脆弱性診断方法は、お客様保有のAmazon EC2環境に対して、イージスEWを実施しました。



**調査対象のサーバはAmazon EC2上に構築されており、
DNSサーバはAmazon Route 53にて提供されいます。**

事例3　SSO認証基盤サービス会社様

未来研究所 Future Research Inc.

■イージスEWによる診断内容

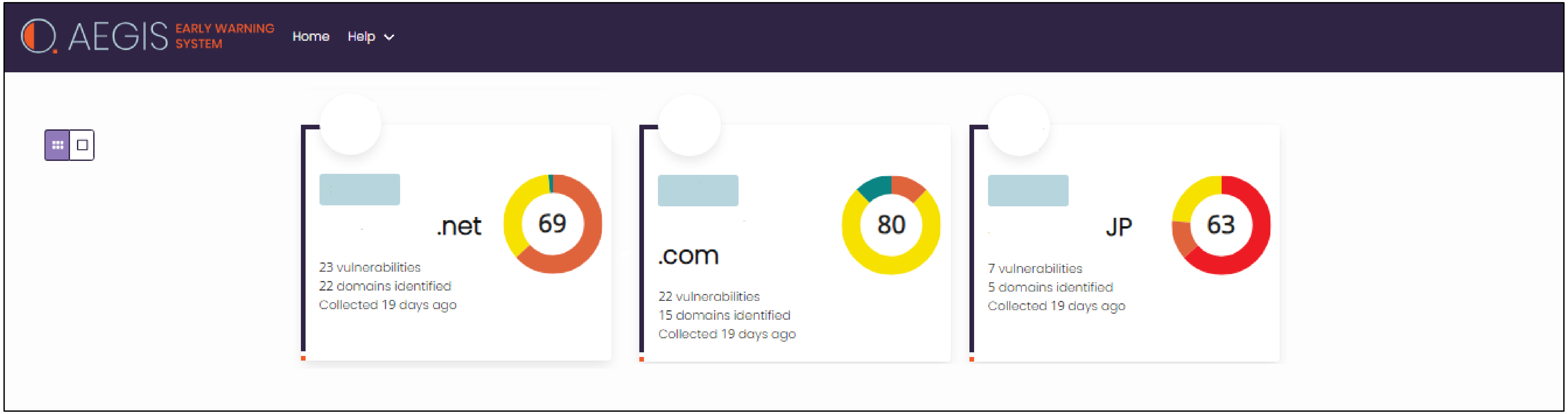
この導入事例では、AMSフルスキャンを行いました。
「メールなりすまし対策」、「データ侵害」、「サーバ証明書」、
「ポート調査」、「HTTPセキュリティヘッダ」、「CVE調査」を実施しました。

分野識別	Mail	送信ドメイン認証	「メールなりすまし」対策できているかどうか？
	BREACH	データ侵害	お客様のドメインで登録されたメールアドレスが、 ダークウェブに流れていないか？
	WEBCERT	Web認証関連	WEBサーバ証明書は正しいのか？
	HEADER	HTTP関連ヘッダー関連	HTTPセキュリティヘッダは正しく導入されているか？
	PORT	ポートスキャン攻撃	攻撃されやすいポートは開いていないか？
	CVE	共通脆弱性識別子CVE (Common Vulnerabilities and Exposures)	CVE脆弱性が残っていないか？

事例3　SSO認証基盤サービス会社様

■その後の導入結果(1)

イージスEWを導入することにより「お客様専用ダッシュボード」により複数ドメインの一括管理が可能となりました。

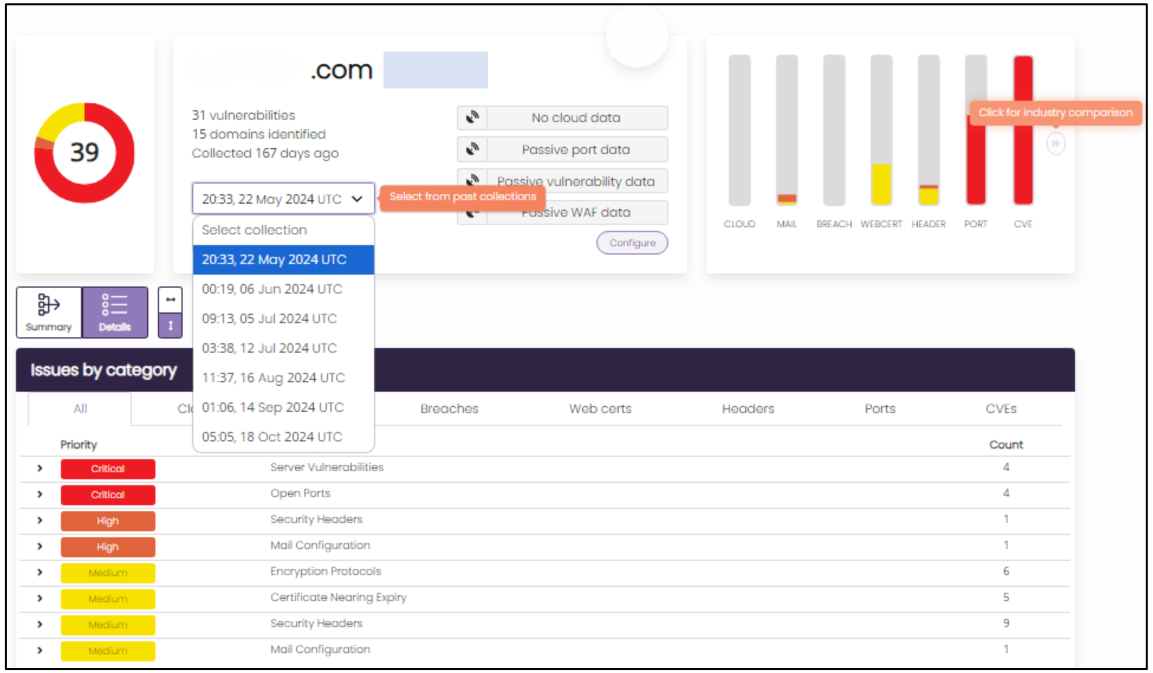


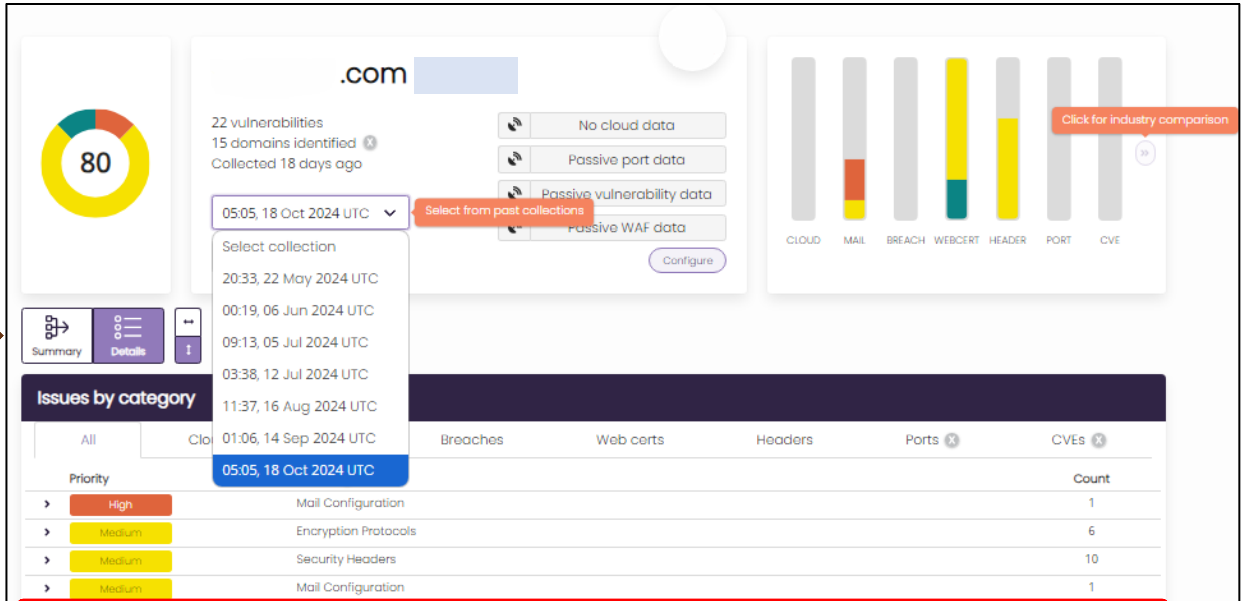
イージスEWでは、エンドユーザ様にダッシュボードを引き渡すことが可能です。
これにより、お客様は「自社で登録したAEGIS-EWアカウント」にて、
「自社用のダッシュボード」を運用できます。

事例3　SSO認証基盤サービス会社様

■その後の導入結果(2)

当初、本番環境に対して既知のポートやCVEを含む脆弱性が残ったままでした。
イージスEW導入から、５ヶ月でこれらの脆弱性は解消されました。





５ヶ月で、既知ポートと脆弱性がゼロ達成！

古いOpenSSH(OpenSSH 9.3以前のバージョン）に由来する脆弱性が多数ありました。
現在、この脆弱性は解消されハードニングができている状態になりました。

事例４　化粧品製造業様

事例４　化粧品製造業様

未来研究所
Future Research Inc.

■お客様の概要

お客様は、大手化粧品販売会社に化粧品を製造販売している製造業様です。
なお、このお客様では複数のドメインを所有しており、セキュリティコンサルティングも希望しておりました。

株式会社　＊＊＊＊＊＊
資本金：　1000万
社員数：　300名
年商：　100億円

主な納入先：　大手化粧品販売会社
自社ブランド販売サイトも所有

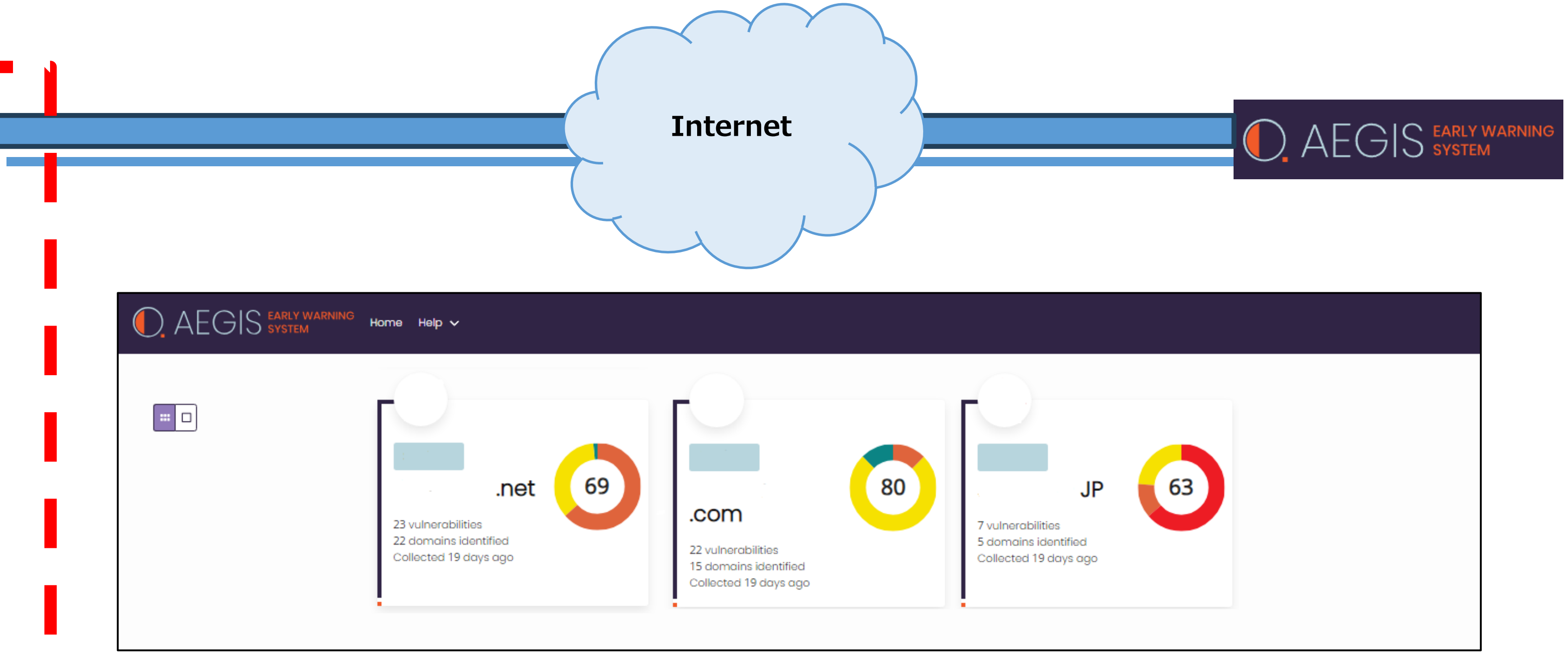
イージスEW導入の理由：
自社ブランドのホームページに対するハードニング
自社生産管理システム対するハードニング

事例４　化粧品製造業様

未来研究所
Future Research Inc.

■脆弱性診断実施方法

今回の事例では、複数のドメインが、複数のホスティング先に分散されたおりました。
このため、先に紹介した「お客様専用ダッシュボード」による管理機能が有効に機能しました。



複数のホスティング先に、複数のドメインが紐付いています。
このような場合には、専用ダッシュボードによる総合的な脆弱性管理が重要になります

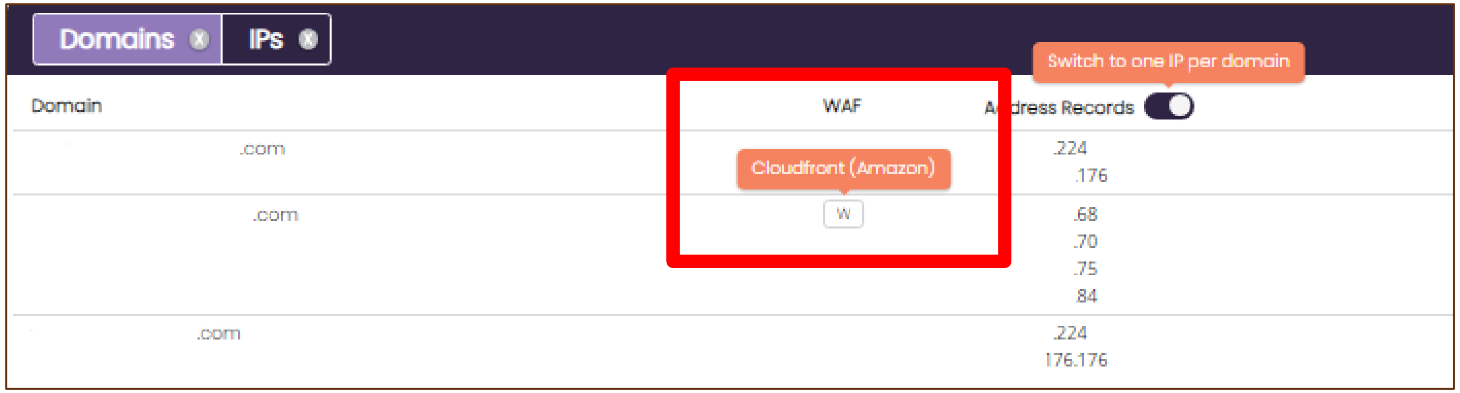
事例４　化粧品製造業様

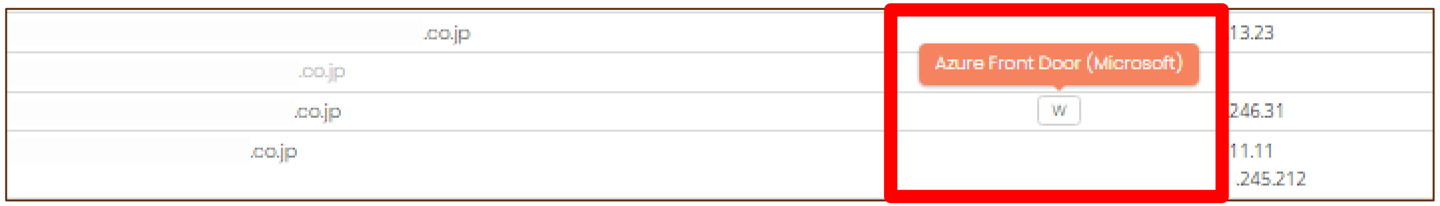
未来研究所
Future Research Inc.

■その後の導入結果(1)

イージスEWでは、お客様環境にWAFが導入されている場合には、「自動的に検出」して、お客様プラットフォームを特定します。これにより、お客様によるプラットフォーム調査時間を大幅に短縮することが可能です。

また、イージスEWは、AWSやAzureプラットフォーム診断機能をペネトレーションモードとして搭載しております。
AWSやAzureをお使いと一目でわかり、お客様へのペネトレーションテスト提案もスムーズに行うことが可能です。



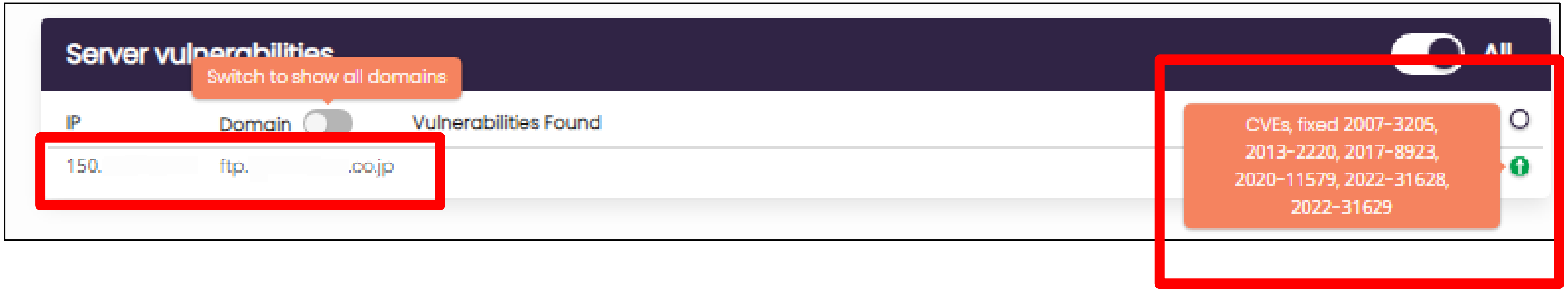


「Amazon Croudfront」、「Microsoft Azure Front Door」だけでなく、Croudflare、F5-BIG IP、AWS Elastic LB、imunify360、lightspeed、Citrixなど多くのWAFプラットフォームを自動検出します。

事例４　化粧品製造業様

■その後の導入結果(2)

当初、本番環境に対して既知のポートやCVEを含む脆弱性が残ったままでした。
イージスEW導入から、４ヶ月目でCVEを解消でこれらの脆弱性は解消されました。



本社FTPサーバに対して、古いPHP(7.1系）に由来する重大な脆弱性(CVSSv3.1 ＝ 9.8緊急）を解消しました。
このお客様は、弊社が定期的にコンサルティングを行って、イージスEWの診断結果に基づく脆弱性解消を継続しております。

Thanks

